

Ballot Marking Device Attack

Taxonomy

Configuration-related, Ballot Database

Applicability

[DRE](#), [DRE with VVPT](#)

Method

Based on assumption of Trojan code placed on voting machine that can successfully manipulate ballot database, and/or voting machine presentation of ballot data.

Resource Requirements

Expertise in voting application, voting system auditing.

Potential Gain

Medium to Low. Each voting machine must be modified; moreover, the exploit is in operation only until the omission is detected and verified by the polling place judges, at which point all machines in polling place would be examined and the tampering discovered and the altered ballots discredited.

Likelihood of Detection

This attack is predicated upon the voter overlooking the omission, and thus is only effective for small, low-awareness proposition issues and races. Most polling places publicly post a sample ballot, as well as offering one in the voter registration process. Local Elections officials also conduct mailing campaigns to inform the voters of the ballot prior to election day. Finally, the exploit must go undetected for the entire voting day (typically 13-14 hours) if the affected votes are to be entered into the official tally.

Countermeasures

[Two-level configuration files](#), Checksums, configuration checking tools, or other ways to detect or prevent alterations to approved configuration profiles.

Preventative Measures

Creating a well informed voting public, by means of public posting of official ballot content and other awareness-raising efforts prior to the day of voting (e.g. activities by the League of Women Voters, and the various political parties).

Detection Measures

A well-trained staff of polling place elections judges. An effective Logic and Accuracy (L&A) Testing protocol would also disclose any ballot alterations, assuming the trojan code enabling this exploit could not mask itself and its changes when the machine was in testing mode.